UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/761,906	01/17/2001	Ronald P. Doyle	RSW920000096US1	6182

7590 03/29/2005

Jeanine S. Ray-Yarletts
IBM Corporation T81/503
PO Box 12195
Research Triangle Park, NC 27709

EXAMINER	
HOFFMAN, BRANDON S	
ART UNIT	**PAPER NUMBER**
2136	

DATE MAILED: 03/29/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/761,906	DOYLE ET AL.	
	Examiner	Art Unit	
	Brandon Hoffman	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *04 March 2005*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-18,20,22-36,41-58,60,62-76,81-98,100 and 102-116* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☒ Claim(s) *23-32,63-72 and 103-112* is/are allowed.

6)☒ Claim(s) *1-18,20,22,33-36,41-58,60,62,73-76,81-98,100,102 and 113-116* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-18, 20, 22-36, 41-58, 60, 62-76, 81-98, 100, and 102-116 are pending in this office action.

2. Applicant's response, filed March 4, 2005, has been considered and are persuasive.

Rejections

3. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

Claim Rejections - 35 USC § 103

4. Claims 1-3, 5-7, 12, 15, 16, 20, 22, 35, 36, 41-43, 45-47, 52, 55, 56, 60, 62, 75, 76, 81-83, 85-87, 92, 95, 96, 100, 102, 115, and 116 are rejected under 35 U.S.C. 103(a) as being unpatentable over Bjorn et al. (U.S. Patent No. 6,125,192) in view of Matchett et al. (U.S. Patent No. 5,229,764)

Regarding claims 1, 41, and 81, Bjorn et al. teaches a method/system/computer program product of providing a secure, integrated device with dynamically selectable capabilities, comprising step of:

- Operating a security core which provides security functions (col. 5, line 43 through col. 6, line 27);
- **Establishing a secure, operable connection of** one or more components to the security core, such that the security core can vouch for authenticity of each securely operably connected component, wherein the security core and the operably connected components thereby comprise the secure integrated device (col. 4, line 39 through col. 5, line 22);
- **Securely performing a transaction using the secure integrated device** (fig. 3);

Bjorn et al. does not teach **detecting whether all components remain operably connected to the secure integrated device during the securely performed transaction; and marking the securely performed transaction as not secure if one or more of the components fails to remain operably connected to the secure integrated device during the securely performed transaction.**

Matchett et al. teaches **detecting whether all components remain operably connected to the secure integrated device during the securely performed transaction** (col. 2, lines 55-66); **and marking the securely performed transaction as not secure if one or more of the components fails to remain operably connected to the secure integrated device during the securely performed transaction** (col. 10, lines 3-5).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine detecting whether all components remain operably connected to the secure integrated device during the securely performed transaction; and marking the securely performed transaction as not secure if one or more of the components fails to remain operably connected to the secure integrated device during the securely performed transaction, as taught by Matchett et al., with the method of Bjorn et al. It would have been obvious for such modifications because these limitations enhance security and prevent user substitution to an unauthorized user (see col. 2, lines 55-66 of Matchett et al.).

Regarding claims 2, 42, and 82, the combination of Bjorn et al. in view of Matchett et al. teaches wherein selected ones of the operable connections are made using one or more buses of the secure integrated device (see fig. 2, ref. num 205/290 of Bjorn et al.).

Regarding claims 3, 43, and 83, the combination of Bjorn et al. in view of Matchett et al. teaches wherein selected ones of the operable connections are made using a wireless connection between respective ones of the components and the security core (see col. 4, lines 18-22 of Bjorn et al.).

Regarding claims 5, 45, and 85, the combination of Bjorn et al. in view of Matchett et al. teaches wherein selected ones of the secure operable connections are provided when the security core is manufactured (see col. 9, lines 52-62 of Bjorn et al.).

Regarding claims 6, 46, and 86, the combination of Bjorn et al. in view of Matchett et al. teaches wherein the components comprise one or more of (1) input/output components and (2) application processing components (see col. 8, lines 4-30 of Bjorn et al.).

Regarding claims 7, 47, and 87, the combination of Bjorn et al. in view of Matchett et al. teaches wherein **establishing a secure, operable connection of one or more components to the security core** further comprises authenticating the operably connected component to the security core (see col. 9, line 30 through col. 10, line 7 of Bjorn et al.).

Regarding claims 12, 52, and 92, the combination of Bjorn et al. in view of Matchett et al. teaches further comprising authenticating the security core to the operably connected component (see col. 9, line 30 through col. 10, line 7 of Bjorn et al.).

Regarding claims 15, 55, and 95, the combination of Bjorn et al. in view of Matchett et al. teaches wherein the secure integrated device is a pervasive computing device (see col. 4, line 65 through col. 5, line 4 of Bjorn et al.).

Regarding claims 16, 56, and 96, the combination of Bjorn et al. in view of Matchett et al. teaches wherein one or more cryptographic keys are securely stored in each component; and wherein at least one of the securely stored keys is used by the step of securely operably connecting each component (see col. 5, lines 22-28 of Bjorn et al.).

Regarding claims 20, 60, and 100, Bjorn et al. teaches a method/system/computer program product of **providing a secure, integrated device with dynamically selectable capabilities, comprising:**

- **Operating a security core which provides security functions** (col. 5, line 43 through col. 6, line 27);
- **Establishing a secure, operable connection of one or more components to the security core, such that the security core can vouch for authenticity of each securely operably connected component, wherein the security core and the operably connected components thereby comprise the secure integrated device** (col. 4, line 39 through col. 5, line 22);
- **Securely performing a transaction using the secure integrated device** (fig. 3);

Bjorn et al. does not teach detecting whether the components remain operably connected to the secure integrated device during the securely performed transaction; and aborting the securely performed transaction if one or more of the components fails

to remain operably connected to the secure integrated device during the securely performed transaction.

Matchett al. teaches detecting whether the components remain operably connected to the secure integrated device during the securely performed transaction (col. 2, lines 55-66); and aborting the securely performed transaction if one or more of the components fails to remain operably connected to the secure integrated device during the securely performed transaction (col. 10, lines 3-5).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine detecting whether the components remain operably connected to the secure integrated device during the securely performed transaction; and aborting the securely performed transaction if one or more of the components fails to remain operably connected to the secure integrated device during the securely performed transaction, as taught by Matchett et al., with the method of Bjorn et al. It would have been obvious for such modifications because these limitations enhance security and prevent user substitution to an unauthorized user (see col. 2, lines 55-66 of Matchett et al.).

Regarding claims 22, 62, and 102, official notice is taken that wherein securely performing a transaction further comprises digitally notarizing, by the security core, an output data stream created by a selected one of the operably connected components of

the secure integrated device. One of ordinary skill in the art would have been motivated to use digital notarization to support non-repudiation and establish trust between entities.

Regarding claims 35, 75, and 115, the combination of Bjorn et al. in view of Matchett et al. teaches wherein the security core is located on a selected one of the operably connected components, and wherein the security core and the selected one are connected to a common bus (see fig. 2, ref. num 205/290 of Born et al.).

Regarding claims 36, 76, and 116, the combination of Bjorn et al. in view of Matchett et al. teaches wherein a second security core is located on a selected one of the operably connected components, and wherein the security core and the second security core each provide security functions for one or more components of the secure integrated device (see fig. 3 of Bjorn et al., "other systems" could contain the security core).

Claims 4, 8-11, 13, 14, 17, 18, 33, 34, 44, 48-51, 53, 54, 57, 58, 73, 74, 84, 88-91, 93, 94, 97, 98, 113, and 114 are rejected under 35 U.S.C. 103(a) as being unpatentable over Bjorn et al. (USPN '192) in view of Matchett et al. (USPN '764), and further in view of England et al. (U.S. Patent No. 6,330,670).

Regarding claims 4, 44, and 84, the combination of Bjorn et al. in view of Matchett et al. teaches all the limitations of claims 1, 3 & 41, 43 & 81, 83, respectively, above. However, the combination of Bjorn et al. in view of Matchett et al. does not teach wherein the performing step uses Secure Sockets Layer encryption to encrypt data or an equivalent which provides mutual authentication of both endpoints, negotiation of a time-limited key agreement with secure passage of a selected encryption key, and periodic renegotiation of the time-limited key agreement with a new encryption key.

England et al. teaches wherein the performing step uses Secure Sockets Layer encryption to encrypt data or an equivalent which provides mutual authentication of both endpoints, negotiation of a time-limited key agreement with secure passage of a selected encryption key, and periodic renegotiation of the time-limited key agreement with a new encryption key (col. 10, lines 4-13).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine using SSL for encryption of both endpoints, as taught by England et al., with the method of Bjorn et al./Matchett et al. It would have been obvious for such modifications because SSL uses session keys, this prevents an attacker from disconnecting and reconnecting at a later time after a device has authenticated itself (see col. 10, lines 4-13 of England et al.).

Regarding claims 8, 48, and 88, the combination of Bjorn et al. in view of Matchett et al./England et al. teaches wherein authenticating **the operably connected component to the security core** provides a unique identifier of the operably connected component to the security core (see col. 9, lines 42-51 of England et al.).

Regarding claims 9, 49, and 89, the combination of Bjorn et al. in view of Matchett et al./England et al. teaches wherein **establishing a secure, operable connection of one or more components to the security core** is activated by a hardware reset of the component, and wherein the hardware reset is activated by operably connecting of the component (see col. 8, lines 3-37 of England et al.).

Regarding claims 10, 50, and 90, the combination of Bjorn et al. in view of Matchett et al./England et al. teaches wherein authenticating **the operably connected component to the security core** is activated during execution of instructions stored on the component, and wherein the execution of the stored instructions is activated by a hardware reset of the component (see col. 8, lines 3-37 of England et al.).

Regarding claims 11, 51, and 91, the combination of Bjorn et al. in view of Matchett et al./England et al. teaches wherein instructions for performing the authenticating **of the operably connected component to the security core** are securely stored on the component (see col. 8, lines 18-22 of England et al.).

Regarding claims 13, 53, and 93, the combination of Bjorn et al. in view of Matchett et al./England et al. teaches wherein authenticating the operably connected component **to the security core** further comprises using public key cryptography (see col. 8, lines 7-8 of England et al.).

Regarding claims 14, 54, and 94, the combination of Bjorn et al. in view of Matchett et al./England et al. teaches wherein authenticating the security core **to the operably connected component** further comprises using public key cryptography (see col. 8, lines 7-8 of England et al.).

Regarding claims 17, 57, and 97, the combination of Bjorn et al. in view of Matchett et al./England et al. teaches wherein one or more cryptographic keys are securely stored in the secure integrated device (see fig. 1B, ref. num 164 of England et al.).

Regarding claims 18, 58, and 98, the combination of Bjorn et al. in view of Matchett et al./England et al. teaches further comprising authenticating a user of the secure integrated device (see col. 7, lines 45-50 of England et al.).

Regarding claims 33, 73, and 113, the combination of Bjorn et al. in view of Matchett et al./England et al. teaches further comprising dynamically revising functionality in a selected one of the secure operably connected components of the

secure integrated device by securely applying a firmware update to the selected one and requiring the selected one to re-authenticate itself to the security core, such that the security core can continue to vouch for the authenticity of the selected one (see col. 12, line 66 through col. 13, line 9 of England et al.).

Regarding claims 34, 74, and 114, the combination of Bjorn et al. in view of Matchett et al./England et al. teaches wherein capabilities of the secure integrated device are dynamically revised by subsequent operation of **establishing a secure, operably connection of one or more components to the security core**, the subsequent operation being activated upon operably connecting a new component to the security core, wherein the new component authenticates itself to the security core, with a result of the authentication being that the capabilities of the secure integrated device are thereby augmented with capabilities of the new component (see col. 12, line 66 through col. 13, line 9 of England et al.).

Allowable Subject Matter

5. Claims 23-32, 63-72, and 103-112 are allowed. These claims correspond to claims that were rejected under a double patenting rejection. Applicant filed a terminal disclaimer, which remedied the rejection.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Brandon Hoffman whose telephone number is 571-272-3863. The examiner can normally be reached on M-F 8:30 - 5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Brandon Hoffman

BH

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100